Explanation of Grading Methodology

The computer security grades are based on information contained in agencies' and Inspectors General (IGs) Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget (OMB) for fiscal year 2006.

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is FISMA, which lays out the framework for annual IT security reviews, reporting, and remediation planning at federal agencies. It requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to OMB, Congress, and the GAO.

OMB's 2006 reporting guidance instructed agencies and IGs to summarize the results of annual IT security reviews of systems and programs, agency progress on correcting identified weaknesses, and the results of other work performed during the reporting period using OMB's performance measures to assess and report the status of their agencies' security programs. In addition, agencies were permitted to include additional performance measures they had developed. OMB required agencies to submit their reports by October 1, 2006.

Assignment of grades

In assigning security grades to the agencies, the methodology developed for the fiscal year 2005 FISMA grades was used, with the exception of adjustments required by changes in OMB's FISMA reporting instructions (next paragraph). This approach ensures consistency in the methodology used to assign grades and serves to highlight progress made by an agency if this year's grade indicates improvement.

The weighted scores are based on OMB's performance metrics, with a perfect score totaling 100 points. OMB provided a range of responses for most questions. The number of points assigned to each response is proportional to the extent the element has been implemented. For example, agencies received zero points for a response indicating a percentage that falls below an acceptable threshold (for example: 50% or less of known IT security weaknesses being incorporated in the plan of action and milestones). Proportionally, more points were given for answers that ranged between 51 and 70%, 81 and 95%, etc. The full weighted value was awarded for answers that ranged between 96 and 100%.

For more specific weighting of questions see the scoring methodology.

The scores for the 24 agencies were tallied on the basis of an analysis of agency and IG responses. The final numerical score is the basis for the agency's letter grade. Letter grades for the 24 major departments and agencies were assigned as follows:

90 to 93 = A-	94 to 96 = A	97 to 100 = A+
80 to 83 = B-	84 to 86 = B	87 to 89 = B+
70 to 73 = C-	74 to 76 = C	77 to 79 = C+
60 to 63 = D-	64 to 66 = D	67 to 69 = D+
59 and lower = F		

Major changes to the weighting of grades

Changes in OMB's FISMA reporting instructions from FY05 to FY06 required only minor adjustments to the scoring methodology that was used to determine the FISMA grades. To facilitate future consistency, the following major categories were used: annual testing, plan of action and milestones, certification and accreditation, configuration management, incident detection and response, training and systems inventory. Changes for each area are listed below.

Annual testing – Made minor edits regarding review of contractor systems.

Plan of action and milestones – No changes.

Certification and accreditation – No changes.

Configuration management – No changes.

Incident response and detection – No changes.

Training – Adjusted response ranges to be consistent with reporting template requirements.

Inventory – Adjusted last two inventory questions to reflect reporting template requirements.

Improvements still needed

Although many agencies reported improvements in their implementation of FISMA, such as certifying and accrediting a higher percentage of their systems and maintaining an inventory, much work is still needed to ensure federal information systems are secure. Areas of continued weaknesses include:

Annual Testing

- Agencies continue to report large numbers of uncategorized systems.
- Contractor systems are not always reviewed.

Plan of action and milestones

- Agencies are not effectively using them to prioritize and track weaknesses.

Certification and accreditation

IGs continue to report weaknesses in agencies' C&A processes.

Configuration management

Many agencies have these policies; however, several agencies do not implement them consistently.

Incident Reporting

Agencies continued to show inconsistencies in reporting incidents, with some agencies reporting few or no incidents.

Training

Most agencies have ensured that their employees have received security training and awareness, but they have been less successful in ensuring that those with significant security responsibilities receive specialized training.

Inventory

Some agencies have not developed complete and accurate inventories of their major IT systems.

Overall

Many of the largest agencies continue to have low scores; however, DHS has shown some improvement.